



Timothy Stenovec [Become a fan timothy.stenovec@huffingtonpost.com](mailto:timothy.stenovec@huffingtonpost.com)

[Email](#)

Passwords Are Terrible -- And These Companies Want To Kill Them

Posted: 03/04/2015 2:01 pm EST Updated: 03/06/2015 12:59 pm EST



215

0

36



-
-
-

Imagine sitting down in front of your computer or grabbing your smartphone and being able to seamlessly log in to every account you need. Maybe your device recognizes your fingerprint, your eyes or your heartbeat. It just knows it's you, and not an impostor.

That's the password-free future that many tech companies envision. It just may take them a while to get there.

Passwords have long been the gold standard in online and device security, and we've been using them for as long as we've had to log in to computers and accounts.

The trouble is, passwords are horrible. Many people don't use them properly. While security experts recommend using a strong, unique password for every service, most users don't do that, [leaving them vulnerable to hacking](#). And many of us regularly forget our passwords and have to reset them frequently. But take heart: The race to kill the dreaded password is on. Tech giants are battling to replace it with biometric technology -- using your face, eyes, fingerprint or [heartbeat](#) to identify you -- which could mean more security and convenience for consumers.

This week, Qualcomm, which makes the chips for many Android smartphones, announced Snapdragon Sense ID, a new type of sensor that uses sound waves to detect 3-D details of your fingerprint. The company says the sensor [can read fingers covered in sweat or lotion](#) and can work on glass, steel, plastic and aluminum devices, giving more flexibility to device manufacturers.

Snapdragon Sense ID, unveiled this week at Mobile World Congress, an annual gathering in Barcelona for tech and telecom leaders, is just one of several new developments in biometric security that technology companies have announced of late.

Also at Mobile World Congress, Samsung said that it had [improved the fingerprint sensor](#) on its new high-end smartphones.

At the Consumer Electronics Show in January, chipmaker Intel unveiled [True Key](#), which uses facial recognition, fingerprint scanning and other authentication methods to unlock a password manager that gives access to apps and online accounts.

And Touch ID, Apple's fingerprint-sensing technology for newer iPhones and iPads -- widely seen as the most successful application of biometric security to consumer devices -- is available on a growing number of third-party apps.

"There's somewhat of a perfect storm happening in the marketplace now," said Anthony Antolino, the chief marketing and business development officer at [eyeLock](#), a New York-based company that has built iris authentication platform technology.

Antolino said that frequent high-profile security breaches, the availability of less expensive and smaller biometric technologies and the staggering rise in the number of mobile devices are all driving the urge to end the password age.

The success of Apple's Touch ID in particular has inspired the rest of the industry to follow, according to [Chester Wisniewski](#), a senior security advisor at the security company Sophos.

In September 2013, Apple released Touch ID on the iPhone 5S as an alternative to unlocking the phone with a passcode. The company said at its developer conference last June that before Touch ID was

available, fewer than half of iPhone owners used a passcode. But as of that conference, 83 percent of iPhone 5s users were using Touch ID to unlock their phones.

“Apple proved a business model offering consumers biometrics,” Wisniewski said. “Apple went out there and proved people will use it if it’s easy enough to use.”

A year later, Apple [opened up Touch ID to non-Apple apps](#), so people can now use their fingerprints to log in to some services, like Amazon and personal finance manager Mint. And people with the latest Apple devices can also use Touch ID to pay for things with their phones. Still, it will be quite a while before the password is out of our lives completely.

One issue is the reliability of biometric security. Even though Touch ID is widely seen as successful, it doesn’t work well for everyone. It also may not work if your hands are cold or after you’ve showered or done the dishes.

When Intel [debuted True Key during a keynote address at the CES](#), the program failed to recognize the presenter during the demonstration.

Passwords have no such issues. Despite their drawbacks, they work -- if you type in your password correctly, you’ll get in.

Another issue is trust: Consumers must believe that these companies are taking good care of data on their fingerprints, faces and eyes.

Wisniewski lauded Apple for [the way it protects the privacy of users' fingerprints](#), but said consumers shouldn’t expect the same levels of security from every company that holds their biometric data -- especially when protecting password data has already proven to be so difficult.

“Why should we trust that the companies asking us for our biometric data are going to be any better with it than my password?” Wisniewski said.

For the time being, security experts [recommend](#) using [password managers](#) -- digital lockers that not only generate strong, unique passwords, but also store them -- that can be unlocked with one strong password. They also recommend using multi-factor authentication, which requires you to use a code generated on another device, like a smartphone, when it's available.

"Right now we're eliminating the hassle of remember multiple passwords," said Mark Hocking, vice president and general manager of Safe Identity at Intel. "Down the road, we want to eliminate the password completely. But that's going to take a long time."

This post has been updated to more broadly describe the company eyeLock's work.

CORRECTION: This story previously suggested incorrectly that True Key uses a single master password for all of a user's linked accounts. This post also misidentified Mark Hocking as Mark Miller.

The absolute worst passwords you can use and how to choose a better one

March 11, 2015

No Comments

1055 Views

Tech News

Taylor Leddin



Your password might suck

As 2015 gets into full swing, the wrap-ups of 2014 are fading out. Among them, is a list of the worst passwords of this past year and it seems as though the horrible classics are still in use. With everything requiring a password, it is tough to come up with a code/variation of a code to keep up with all of your accounts. However, there are better options than “1234.”

SplashData released their yearly list of most common passwords on the Internet and offered the 25 most frequently used passwords throughout the World Wide Web. It seems as though numbers, superheroes, and the infamous “qwerty” are the hot contenders. The list was acquired from analyzing 3.3 million leaked passwords in 2014.

Mark Burnett, an online security expert, helped SplashData compile their list and says that the list shows people are becoming more aware of better password usage than they have been in years prior. He also mentioned that the top 25 only accounts for 2.2 percent of the exposed passwords.



We're vulnerable online, but you can do something about it

The full list includes:

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 1234567890
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

With continuous proof of our online privacy being extremely vulnerable, it is important to create passwords that will protect you. While there is a fine-line between astoundingly easy and incredibly fool-proof (i.e. the time that I got an e-mail saying someone in Russia tried to hack my Gmail account so I changed my password to a 50-word phrase and have been regretting it ever since), coming up with a safe password may be easier than you think.

Choose a proper password

For example, base your password on something you like. Say you're a fan of The Rolling Stones. You can make the band your theme for passwords and change up the variation depending on security requirements. You can do: rollingstones1,

Rolling1Stones, YouCantAlwaysGetWhatYouWant, etc. If you have a theme for passwords, it may be easier for you to keep track of what goes where.

However this may still be tricky to keep track of and further assistance may be required. For this, I would suggest the use of LastPass. It is a free, online tool that allows you to store all of your passwords in one password-protected place. LastPass also offers “Enterprise” which is password security for a company.

Whichever route you choose, know that it is possible to keep yourself safe on the Internet. *And let us all make a pact to eliminate the usage of “1234” and “qwerty”.*

Source: <http://agbeat.com/tech-news/the-absolute-worst-passwords-you-can-use-and-how-to-choose-a-better-one/>

Mobile operators want to do away with online passwords

Everyone needs ID. (Reuters/Jonathan Alcorn)

SHARE

WRITTEN BY

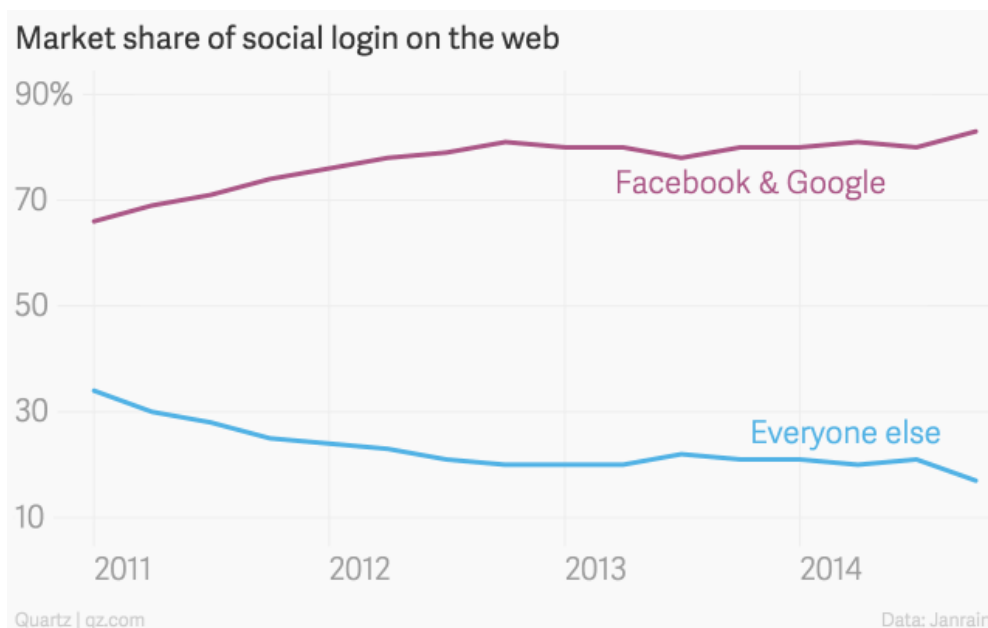
[Leo Mirani](#)@lmirani

OBSESSION

[Mobile Web](#)

March 6, 2015

Nobody likes passwords. They're hard to remember, [we're terrible](#) at coming up with good ones, and they're [not much use](#) anyway. Yet they refuse to go away. The closest we've come to [getting rid of them](#) is by using the likes of Google and Facebook to log in to other websites. At least that reduces the number of passwords and login details we have to manage.



That's just fine with Facebook and Google, which in the process of making internet users' lives easier have become custodians of our online identities. Between them, the two web giants control more than 80% of the “social login” market, as third party sign-in is called. That grants them access to [valuable data](#) about what people are doing as they travel around the web.

Mobile operators have had enough of it. As data rather than voice or text becomes the big reason people use their mobile phones, networks want to extract more value from their users. At the moment, operators are mostly just the pipes through which data flow. But just as they made money from ancillary “value added services” such as caller-back tunes and ring tones, they want to put the data to good use.

Identity is one way of doing that. And operators are counting on eliminating passwords as their ticket. Over the past year, the industry trade body, GSMA, has been rolling out [Mobile Connect](#), a service that ties peoples' identities to their phones rather than to a password. Here's how it works:



As Mark Little of the GSMA puts, the hope for mobile connect is that it “makes mobile operators more relevant in the ecosystems where they weren't relevant.”

Some 17 operators in 13 countries have already [signed up](#) for the service, mostly in Asia and Africa, in countries including Bangladesh, China, Indonesia, Malaysia, Cote D'Ivoire, Gabon, and Nigeria.

Many existing internet users are unlikely to stop signing into websites with Google and Facebook; it is more difficult to get people to change their behavior than it is to convince them to start off differently. But as hundreds of millions of people come online for the first time in the developing world—almost entirely through mobile phones—mobile operators finally have a chance to wrest back some control of online identity from Google and Facebook.

Source: <http://qz.com/357354/mobile-operators-want-to-do-away-with-online-passwords/>